GIZMODO

Before You Hit 'Submit,' This Company Has Already Logged Your Personal Data

Kashmir Hill and Surya Mattu
6/20/17 2:23pm

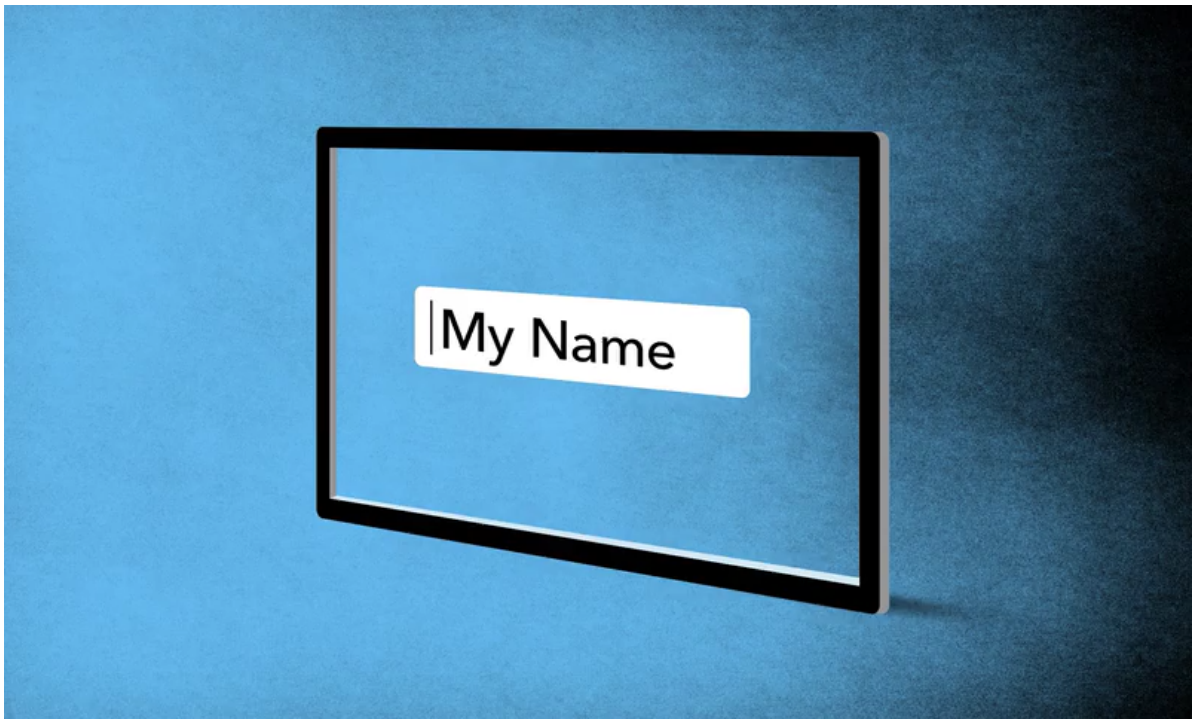


Image by Jim Cooke

If you're daydreaming about buying a home or need to lower the payment on the one you already have, you might pay a visit to the Quicken Loans mortgage calculator. You'll be asked a quick succession of questions that reveal how much cash you have on hand or how much your home is worth and how close you are to paying it off. Then Quicken will tell you how much you'd owe per month if you got a loan from them and asks for your name, email address, and phone number.

You might fill in the contact form, but then have second thoughts. Do you really want to tell this company how much you're worth or how in debt you are? You change your mind and close the page before clicking the Submit button and agreeing to Quicken's privacy policy.

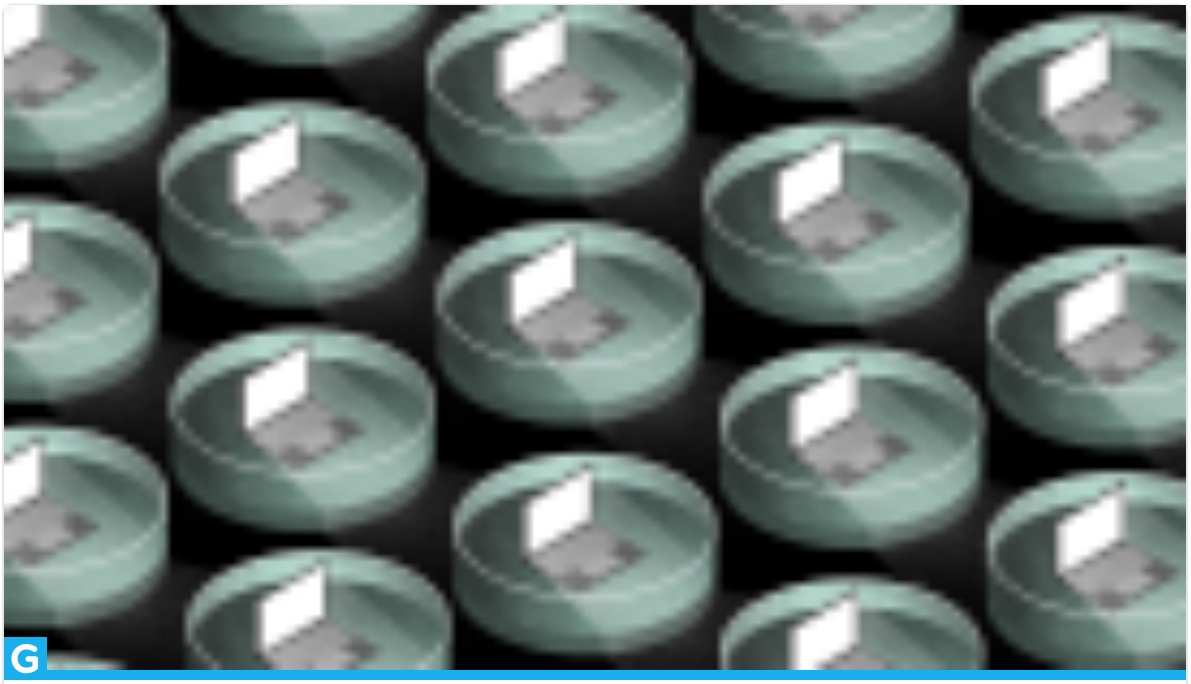
But it's too late. Your email address and phone number have already been sent to a server at "murdoog.com," which is owned by NaviStone, a company that advertises its ability to unmask anonymous website visitors and figure out their home addresses. NaviStone's code on Quicken's site invisibly grabbed each piece of your information as you filled it out, before you could hit the "Submit" button.

During a recent investigation into how a drug-trial recruitment company called Acurian Health tracks down people who look online for information about their medical conditions, we discovered NaviStone's code on sites run by Acurian, Quicken Loans, a continuing education center, a clothing store for plus-sized women, and a host of other retailers. Using Javascript, those sites were transmitting information from people as soon as they typed or auto-filled it into an

online form. That way, the company would have it even if those people immediately changed their minds and closed the page. (It's yet another way auto-fill can compromise your privacy.)

NaviStone is an Ohio-based startup in the business of identifying "ready to engage" customers and matching "previously anonymous website visitors to postal names and addresses." It says it can send postcards to the homes of anonymous website shoppers within a day or two of their visit, and that it's capable of matching "60-70% of your anonymous site traffic to Postal names and addresses."

In yesterday's report on Acurian Health, University of Washington law professor Ryan Calo told Gizmodo that giving users a "send" or "submit" button, but then sending the entered information regardless of whether the button is pressed or not, clearly violates a user's expectation of what will happen. Calo said it could violate a federal law against unfair and deceptive practices, as well as laws against deceptive trade practices in California and Massachusetts. A complaint on those grounds, Calo said, "would not be laughed out of court."



How a Company You've Never Heard of Sends You Letters about Your Medical Condition

In the summer of 2015, Alexandra Franco got a letter in the mail from a company she had never heard ...

Read more

There are at least 100 sites using NaviStone's code according to Builtwith.com, a service that tells you what technologies sites employ. We visited dozens of them to see the code in action. The majority of sites captured visitors' email addresses only, but some sites also captured their home addresses and other entered information.

(To see it in action for yourself, check out our tutorial at the end of this post.)

Only one site of the dozens we reviewed,

Gardeners.com, explicitly revealed in its privacy policy what it was doing. It read, “Information you enter is collected even if you cancel or do not complete an order.” The rest of the sites had the usual legalese in their policies about using standard tracking tech such as cookies and Web beacons, which did not describe the way this particular information capture works.

Do you really?

We sent media inquiries to dozens of sites about why and how they are using the information they’re capturing. Two responded. Quicken Loans did not respond to multiple media inquires.

Road Scholar, a non-profit that arranges educational travel and had NaviStone’s code on its site collecting email addresses before users hit “submit,” told us it uses the NaviStone tool on its website “primarily

to re-activate inquirers who have already expressed an interest in Road Scholar and are already on our mailing list."

A spokesperson for home goods company Wayfair, which was using the Navistone tool on its clothing site JossandMain.com to collect email addresses, told us that the company is "committed to upholding the highest standards for responsible marketing practices across all channels."

"We do not email users who have not formally submitted their email address to our site," Wayfair spokesperson Susan Frechette wrote in an email. "We work with NaviStone to support our direct mail programs."

We asked whether email addresses are collected in order to identify the person and try to find out their home address in order to send them direct mail. Email addresses, after all, much like mobile phone numbers and social security numbers, have become a unique identifier that can be used as a key to unlock other information about us. Frechette declined further comment and referred us to NaviStone.

NaviStone wasn't keen to reveal how it unmasks anonymous website visitors, saying that its technology is proprietary and awaiting a patent. Allen Abbott, NaviStone's chief operating officer, wrote via email that NaviStone doesn't "use email addresses in any way to link with postal addresses or any other form of PII." He said the company's primary business is helping their clients send personalized direct mail.

“Rather than use email addresses to generate advertising communications, we actually use the presence of an email address as a suppression factor, since it indicates that email, and not direct mail, is their preferred method of receiving advertising messages,” Abbott wrote.

At least one other company is known to monitor the things you don’t send: Facebook takes note of the existence of status messages that you compose but don’t post. But this goes beyond that. In some cases, the companies using NaviStone code didn’t have an existing relationship with their visitors and were collecting contact information those consumers had ultimately decided not to give them.

We decided to test how the code works by pretending to shop on sites that use it and then browsing away without finalizing the purchase. Three sites—hardware site Rockler.com, gift site CollectionsEtc.com, and clothing site BostonProper.com—sent us emails about items we’d left in our shopping carts using the email addresses we’d typed onto the site but had not formally submitted. Although Gizmodo was able to see the email address information being sent to Navistone, the company said that it was not responsible for those emails.

Businesses seem to be doing all they can to strip away consumers’ ability to anonymously browse the Web, sacrificing privacy at the altar of commerce. And it’s illustrative of the way your sense of control online can be an illusion, the “submit” feature becoming just another placebo button.

As a result of our reporting, though, NaviStone says it will no longer collect email addresses from people this way.

“While we believe our technology has been appropriately used, we have decided to change the system operation such that email addresses are not captured until the visitor hits the ‘submit’ button,” Abbott wrote.

Alternatively, if you don’t trust sites not to collect your information this way, consider using a tool such as UBlock Origin that prevents invisible claws from descending into the toy chest of data in your browser.

***

Want to see this happen for yourself?

Web browsers have developer tools that let you see what information a website is transmitting and receiving—both the visible and invisible stuff. You can use these developer tools to see this trick. These instructions are for Chrome but the same basic technique should work on Firefox and Safari too, with small differences in the interface.

1. In the Chrome menu, go to “View,” then “Developer,” and select “Developer Tools.”

2. The developer tools should pop up either from the bottom of your browser or the side. To see all the data coming and going from the browser, select the Network tab. You just want to monitor the traffic between the browser and murdoog.com, a website affiliated with NaviStone, to which it is sending the captured information. In the filter in developer tools, type “murdoog.”

3. After our reporting, NaviStone stopped collecting information pre-Submit on most of the sites it was working with. But as of publication time, it was still active on the Quicken Loans mortgage calculator contact page, so head there to check it out.

4. You have to choose “Refinance” or “Purchase” and then hand over some financial information. If you qualify, you’ll get to a contact page and need to fill in the requested information: name, phone number, and email address. Be creative because this information is going to be captured. Each time you hit the tab button, or move to a new field, you should see data being sent to murdoog.com. (If not, you may have a blocker enabled.)

5. Click on the data just sent, click “Headers,” and scroll down to “Query String Parameters,” which are the specific pieces of information your browser is sending to the server. To view these parameters, make sure you’re on the Headers tab and scroll all the

way to the bottom. There will be separate, seemingly random strings listed under the labels v, m, se, and d. The longest of these, labeled d, is the one you want. It will look something like this:

eyJ2IjoiZjZkOTlhYjUtYzdkMy00MGZmLTljN2EtMGEwZDRlM2U4OGEy
IiwibSI6IjAwNDE4NDk5LTc3NDAtNDkwYy1hZWMzLTYzN2RhYWY3Z
TY4MCIsImNzaSI6MzE1MTAzMjI0OSwic2UiOiIyYWZkOGIzMS0xOGY1
LTQzNmMtYjgxZS03MGVjZTg4M2QxNDEiLCJwIjoiOTkyYjE4MGItNGU
1Ny00YzZiLWFmOWUtODA1OTYyMTJiMjg2IiwidSI6Imh0dHBzOi8vd3
d3LnF1aWNrZW5sb2Fucy5jb20vbXktbW9ydGdhZ2UvY2FsY3VsYXRvcj
9xbHNvdXJjZT1uYXYjIS9wdXJjaGFzZS9xdWVzdGlvbi9kb3duLXBheW1l
bnQiLCJwbiI6Ii9teS1tb3J0Z2FnZS9jYWxjdWxhdG9yIiwidCI6Ik15IE1vc
nRnYWdlIENhbGN1bGF0b3IgfCBRdWlja2VuIExvYW5zIiwiYyI6Imh0dH
BzOi8vd3d3LnF1aWNrZW5sb2Fucy5jb20vbXktbW9ydGdhZ2UvY2FsY3
VsYXRvciIsInByIjoiQ0Q0MTQzIiwiZWlkIjoibnNfc2VnXzAwMCIsInMiOj
MsInZzIjoxLCJsIjoiQWN0aW9uIiwidjAxIjoiRm9ybUlucHV0IiwidjAzIjoi
YW5zd2Vyc1twdXJjaGFzZVByaWNlXXxwdXJjaGFzZVByaWNlIiwidjA0Ij
oiMTUwLDAwMCJ9

6. That incomprehensible-looking block of text is encoded using a common web technique called Base64 encoding. Usually it's used to convert binary data like images into strings of text, making them easier to send. Copy the text after the "d:" as shown below and paste it into this online converter.

7. What you should see amid everything else is the information you just typed into the form. It was sent to murdoog.com, a site registered to NaviStone.

This story was produced by Gizmodo Media Group's Special Projects Desk. Email senior reporter Kashmir Hill at kashmir.hill@gizmodomedia.com and data reporter Surya Mattu at surya.mattu@gizmodomedia.com.

ABOUT THE AUTHORS

Kashmir Hill **Kashmir Hill**

Kashmir Hill is the deputy editor for the Special Projects Desk, which produces investigative work across all of Gizmodo Media Group's web sites. She writes about privacy and technology.

Surya Mattu **Surya Mattu**

Surya Mattu is the data reporter at the Special Projects Desk which produces investigative work across all of Gizmodo Media Group's web sites.